ABSTRACT OF THE DISCLOSURE

An object of this invention is to eliminate the necessity to manage a plurality of keys even when image data, in which each tile as an encoding unit is constituted by a plurality of partial encoded data, and the partial encoded data have a hierarchical structure, is encrypted using different encryption keys for the respective partial encoded data. For this purpose, in this invention, a code stream c in which each tile as a compression-coding unit is constituted by a plurality of partial encoded data is received. An encryption tile part designation section repeatedly forms one tile group from a plurality of adjacent tiles and another tile group from adjacent tile groups to define the hierarchical structure of the tiles and tile groups. For a plurality of partial encoded data that constitute the encoded data of a tile located at the terminal of the hierarchical structure, the partial encoded data are arranged toward the terminal in ascending order of priority in decryption to define a tree structure that nodes the respective tile groups, tiles, and partial encoded data. At this time, the encryption tile part designation section determines which partial encoded data of which tile in which layer should be encrypted and outputs encryption tile information ta. A key matrix generation section (12) generates an encryption key ck for the whole of the received code stream c,

sequentially generates the encryption key of each node in the hierarchical structure, and outputs the result as a key matrix ka. An encryption section (13) encrypts the partial encoded data of a tile to be encrypted by using the key generated for that partial encoded data and outputs a code stream c'.